Amendments to the Drawings

Please replace the drawings currently on file with the replacement drawings submitted herewith.

REMARKS

Applicant wishes to thank the Examiner for reviewing the present application.

Drawings

In the Office Action, the Examiner maintained that the drawings on file are not acceptable, and referred to the drawing informalities noted in the Office Action mailed February 24, 2004.

In the above-noted paper, the drawings were objected to because: 1) Figure 1 should be designated as prior art; and 2) The label "Substitute Sheet" at the bottom of the figures should be deleted.

Regarding item 1, Applicant respectfully disagrees. Figure 1 illustrates a data communication suitable for implementing the present invention. The description does not state that Figure 1 illustrates part of the prior art. Applicant believes that it would be improper to label Figure 1 as "prior art", when the components of Figure 1 are referred to in the description in describing an embodiment of the present invention. Applicant respectfully requests that Figure 1 be held acceptable without a label such as "Prior Art".

Regarding item 2, Applicant advises that replacement drawings were submitted with the response dated August 20, 2004 thereby overcoming the informality referred to therein. However, Applicant has re-submitted replacement drawings with the appropriate "Replacement Sheet" label in the respective upper margins.

Accordingly, Applicant believes the drawings submitted herewith overcome the informalities raised in the above-noted paper, and as such, are acceptable.

Claim Objections

Claim 6 was objected to because of a clerical error on line 1 of the claim. Accordingly, the term "operating" has been amended to read "operation" as suggested by the Examiner, to overcome the objection.

Claim Rejections

Claims 1-5 were rejected under 35 U.S.C. 112, second paragraph, as being indefinite, due to the expression "substantially equal" in claim 1. The expression "substantially equal" has been replaced with "similar", and is believed to overcome the rejection under 35 U.S.C. 112, second paragraph.

Claims 1-9 were rejected under 35 U.S.C. 101 for being directed to non-statutory subject matter. Independent claims 1 and 6 have been amended and are believed to define statutory subject matter.

In claim 1, the preamble has been amended to clarify the nature of the method recited. Particularly, the preamble recites a method for generating a result of a group operation. The method is said to be performed by a computing apparatus an integral number of times on a selected element of a group, the group defined as having a plurality of elements including a group identity element. The claim then recites the steps performed to generate the result, namely steps a) to d). A further step, step e) has been added to indicate that the result is output for use in subsequent computations.

Accordingly, claim 1 defines a set of steps that are performed by a computing apparatus in order to generate a result, and the result is then output for subsequent computation. The claim also defines the elements from which the result is generated, namely the selected element of a group having a plurality of elements.

Therefore, Applicant believes that claim 1 is directed to a concrete and tangible method that defines a set of steps performed by a computing apparatus to create a result. The result is generated and output for use in subsequent computations. Applicant respectfully submits that claim 1 defines statutory subject matter and thus complies with 35 U.S.C. 101.

Claims 2-5 are either directly or indirectly dependent on claim 1, and as such, are also believed to be directed to statutory subject matter. Applicant advises that claim 2 has been amended to correct a spelling error.

In claim 6, the preamble has also been amended to clarify the nature of the method recited, indicating that a result is generated and that the method is performed using a cryptographic processor to execute the subsequently recited steps. Consistent with claim 1, claim 6 also provides an output of the result for subsequent computations.

Therefore, Applicant respectfully submits that claim 6 also provides a concrete and tangible method defining a set of steps performed by a computational device (i.e. the cryptographic processor), and as such, is directed to statutory subject matter and thus complies with 35 U.S.C. 101.

Claims 7-9 are either directly or indirectly dependent on claim 6, and as such, are also believed to define statutory subject matter. Applicant advises that claim 7 was amended to correct a clerical error.

In view of the foregoing, Applicant submits that claims 1-9 are directed to statutory subject matter, and thus comply with 35 U.S.C. 101. Therefore, Applicant requests early reconsideration and allowance of the present application.

Respectfully submitted,

John R.S. Orange
Agent for Applicant
Registration No. 29,725

Date: July 22, 2005

BLAKE, CASSELS & GRAYDON LLP
Suite 2800, P.O. Box 25
199 Bay Street, Commerce Court West
Toronto, Ontario M5L 1A9
CANADA

Tel: 416.863.3164
JRO/BSL
21425428.1